3. *Черкасова Е. С.* Профайлинг как метод создания психологического портрета потенциального преступника на этапе организации предварительного расследования // Юр. наука и практика. 2013. С. 72–75.

4. *Fernando S. A.*, *Yukawa T.* Securing Information Sharing Through User Security Behavioral Profiling // Transactions on Engineering Technologies. 2013. С. 655–670.

УДК 004.056

А. И. Полтавец, И. П. Петров, А. С. Федотова, Н. Е. Девицкий
Научный руководитель: ст. преп. И. П. Петров
Тюменский государственный университет, Тюмень

ПРОБЛЕМЫ БЕЗОПАСНОСТИ RECAPTCHA'S

Аннотация. CAPTCHA — это первая линия защиты Интернета от автоматического создания учетной записи, автоматического спама и прочее. Google reCaptcha, одна из самых популярных captcha-систем, в настоящее время используется сотнями тысяч сайтов для защиты от автоматических ботов, проверяя, действительно ли пользователь — человек. Но возможен ли обход CAPTCHA? В этой статье мы хотели бы представить unCaptcha, автоматизированную систему, которая может решать самые сложные reCaptcha, построенную на звуковом анализе, с высокой степенью точности.

Ключевые слова: captcha; reCaptcha; антиспам; информационная безопасность; боты.

Введение

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей [1].

Captchas широко используются на различных веб-ресурсах как защита от автоматических ботов и атак Sybil [2], а также для предотвращения спама. Например, многие онлайн-платформы при покупке билетов [3] требуют, чтобы пользователь решил captcha во время регистрации для предотвращения автоматического создания поддельных счетов.

Безопасность captchas имеет первостепенное значение для защиты веб-ресурсов в Интернете от этих атак. Поскольку распространение новостей и информации все чаще зависит от пользовательского контента на сайтах, таких как Twitter, Facebook, YouTube и многих других, злоумышленники, которые могут обойти систему CAPTCHA и зарегистрировать непропорциональное

количество учетных записей, теоретически могут контролировать информационный поток [4]. Поэтому неудивительно, что в течение многих лет captchas были атакой для исследователей и нападавших [5].

Тем не менее пользователи с нарушением зрения неспособны решить эти визуальные CAPTCHA, что побуждает к созданию «audio captchas». Типичные аудиокапчи состоят из разных дикторов, говорящих слова или цифры со случайными интервалами с переменной скоростью, часто с акцентом и искажением или шумом [5]. Чтобы решить капчу, пользователь должен правильно идентифицировать цифры или слова, произнесенные в аудиоклипе.

Мы представляем unCaptcha, полностью автоматизированную атаку на Google 2017 reCaptcha. unCaptcha не требует высокий уровень ресурсов; вместо того, чтобы проводить собственный анализ локально, unCaptcha использует бесплатные общедоступные сервисы распознавания речи и выполняет минимальное фонетическое преобразование для повышения точности.

Данная статьи организована следующим образом:

– В следующем разделе мы обозреваем систему reCaptcha Google.
– В разделе 2 описывается схема работы unCaptcha.
– В разделе 3 анализируем и оцениваем unCaptcha.

1. Сервис безопасности reCaptcha Google

reCaptcha — это сервис, предлагаемый Google, чтобы определить, действительно ли пользователь веб-сайта является человеком. reCaptcha, предназначена для защиты от автоматизированного создания учетной записи.

reCaptcha опирается на множество различных действий, например, как пользователь вводит текст, перемещает свою мышь и т. д. Если система не уверена, что пользователь является человеком, то она будет предоставлять более сложные задачи. По умолчанию пользователю, не имеющему предыстории с сервисами Google или когда reCaptcha не может определить, является ли пользователь человеком, сервис автоматически предоставляет пользователю сетку изображений, такую как (рис. 1):

Рис. 1. Пример Google reCaptcha

Тем не менее reCaptcha не решаются всеми пользователями; для поддержки пользователей с нарушенным зрением reCaptcha позволяет запрашивать аудиокапчи с помощью значка наушников в нижней левой части вышеприведенного изображения. Эти звуковые вызовы состоят из последовательности записанных голосов, говорящих «девять … пять …

один …» Пользователей, просто просят ввести цифры, которые они слышат. На это и нацелена наша атака.

2. Схема работы unCaptcha

Ключевым фактором, лежащим в основе unCaptcha, является то, что сегодняшние сервисы «речь — текст» обладают высоким потенциалом. Даже собственные бесплатные сервисы Google для речи могут быть использованы против механизма защиты, который они предлагают!

Вкратце схема работы unCaptcha (рис. 2) заключается в следующих шагах:

1. Скачивание аудиокапчи.
2. Полученную аудиокапчу разбить на отдельные сегменты.
3. Загрузить каждый сегмент в несколько онлайн-сервисов «речь — текст».
4. Фонетическое преобразование, подсчет одинаковых и выбор цифры.
5. Объединение сегментов в результат и отправка в reCaptcha Google.

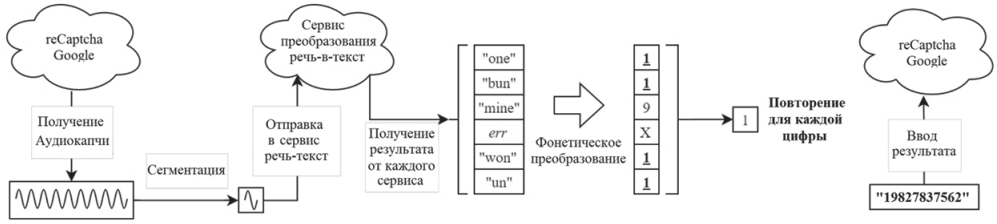

Рис. 2. Схема работы unCaptcha

3. Итоги unCaptcha

Безусловно, уже сейчас можно сказать о том, что если злоумышленники смогут с большей вероятностью обходить капчи, то в Интернете будет огромное количество ботов и рассылки спама. Реализация системы unCaptcha обеспечить защиту сайтов от ботов и одновременной оцифровки текстов. Как один из вариантов защиты можно рассматривать усложнение алгоритма проверки пользователя с отслеживанием множества различных параметров.

Список литературы

1. Капча // Wikipedia [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Капча (дата обращения: 03.11.2017).

2. The Sybil attack in IPTPS, 2002 // Slide Serv [Электронный ресурс]. URL: https://www.slideserve.com/onslow/the-sybil-attack-j-r-douceur-iptps-2002 (дата обращения: 03.11.2017).

3. Google reCaptcha // Google [Электронный ресурс]. URL: https://www.google.com/recaptcha/intro/ (дата обращения: 03.11.2017).

4. Online Human-Bot Interactions: Detection, Estimation, and Characterization // arxiv.org [Электронный ресурс]. URL: https://arxiv.org/abs/1703.03107 (дата обращения: 04.11.2017).

5. *Tam J.*, *Simsa J.*, *Hyde S.*, *Von Ahn L.* Breaking audio captchas // NIPS. 2008.

УДК 004.8

И. А. Пятницкий
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ШИФРОВАНИИ

Аннотация. Криптография стала важнейшим компонентом контроля за аутентификацией, интеграцией, конфиденциальностью и надежностью хранения личных данных, передаваемых через публичные сети. С течением времени, в связи с улучшением производительности и скорости работы компьютеров, старые шифры заменяются на новые, более адаптированные. В статье предложено использовать новые нейросетевые подходы к шифрованию данных.

Ключевые слова: нейронные сети; шифрование; информационная безопасность; инженерно-техническая защита информации.

По мере развития новых методов шифрования [1] математика в них становилась все более и более значимой. Благодаря математике криптография достигла такого уровня развития, что количество математических операций в каждом шифре астрономически высоко. Это означает, что современные криптоалгоритмы стали гораздо более устойчивы к криптоанализу, чем некогда используемые, устаревшие методики, для взлома которых было достаточно ручки и бумаги. Классический криптоанализ не способен эффективно взламывать современные шифры.

По этой причине гораздо большее значение приобретают методы, основанные на перехвате данных, закладке жучков, атаках по сторонним каналам, квантовых компьютерах и бандитском криптоанализе.

Атака по сторонним (или побочным) каналам (от англ. *side-channel attack*) — класс атак, направленный на уязвимости в практической реализации криптосистемы. Такие атаки используют уязвимости в физической реализации алгоритмов. Поскольку любой, даже самый сложный алгоритм в конечном итоге реализуется программой, обрабатывается процессором с определенной конфигурацией, таким образом будет обладать определенной спецификой.